ABSTRACT

Methods and arrangements are provided that allow a smart card having digital signing capabilities to support an encryption-based authentication process. In one exemplary method, the smart card is configured to interface with a personal computer. During a set-up process, the personal computer generates a plurality of random values and selectively hashes at least one of the random values. The smart card then digitally signs another one of the random values to produce a corresponding digital signature, for example, using a private key. The personal computer then generates a key based on the digital signature and at least one of the random values, for example, by further hashing the digital signature concatenated with the random number. The resulting key is then used by the personal computer to selectively encrypt data. During a subsequent use, the smart card is required to once again digitally sign the random number to produce a corresponding digital signature. The personal computer then uses the resulting digital signature to compute a key that can be used to decrypt the previously encrypted data.